IN THE UNITED STATES BANKRUPTCY COURT

FOR THE DISTRICT OF DELAWARE

In re:	
FTX TRADING LTD., *et al.*,1	Chapter 11
Debtors.	Case No. 22-11068 (JTD)
Claimant, Amanuel Y. Giorgis Claim Number: 93202	(Jointly Administered) **Objection Deadline: July 15, 2025 at 4:00P.M.**

CLAIMANT 93202'S RESPONSE

IN OPPOSITION TO THE DEBTORS' 176th OMNIBUS OBJECTION

Claimant 93202, by and through the undersigned counsel, hereby submits his response in opposition to the Debtor's 176th Objection. As explained in greater detail below, Claimant was a victim of a sophisticated cryptocurrency scam which resulted in the theft of over 518,000 USDT. Blockchain analysis of Claimant's stolen cryptocurrency reveals that 87,651 USDT of the Claimant's (stolen cryptocurrency was transferred to deposit wallet addresses held on the FTX exchange.

I. BACKGROUND ON VIRTUAL CURRENCY

1. **Virtual Currency**: Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin (or BTC) and Ether (or ETH), are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

2. **Blockchain**: A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's

technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether exists in its native state on the Ethereum network.

3. **Blockchain Analysis**: Blockchain experts can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to investigations for many reasons, including that it may enable investigators to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, blockchain experts use reputable, free open source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies.

4. **Virtual Currency Address**: A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency

can be sent and received. A virtual currency address is associated with a virtual currency wallet.

5. **Intermediary Address:** An "intermediary address" in virtual currency tracing refers to a wallet address used in a virtual currency transaction that acts as a temporary stopping point between the original sender and the final recipient, often employed to obscure the true source or destination of funds by adding an extra layer of complexity to the transaction trail. Essentially, criminal actors use intermediary addresses as "middleman" addresses to obfuscate the flow of funds. The funds are transferred through the middleman/intermediary address for no legitimate purpose. This is especially obvious because each transfer requires fees, meaning it costs the criminal actors money in order to do these transactions.

6. **Virtual Currency Exchange**: A virtual currency exchange ("VCE"), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

7. **Pass-Through Account:** A "pass-through" account is an account primarily used to transfer funds through a VCE's own addresses, often removing the link between the source of funds and the destination. Pass-through accounts often receive, then promptly transfer the funds without exchange activity, which is an unnecessary step that incurs transaction fees without a legitimate purpose. This effectively turns the VCE into a money laundering mixer.

8. **Virtual Currency Wallet**: A virtual currency wallet (e.g., a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to end and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

9. **Unhosted Wallet**: An unhosted wallet, also known as a self-hosted, non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (e.g., a virtual currency exchange) to facilitate a transaction involving the wallet.

10. **Decentralized Exchange**: A decentralized exchange (or "DEX") is a peer-to-peer marketplace where users can trade virtual currencies directly with other traders without centralized intermediaries. Users generally retain control over their virtual currency rather than entrusting a central authority to host funds in a centralized or "hosted" wallet. DEXs are operated by selfexecuting agreements

written in code, known as "smart contracts," which automate the trading process. DEXs will algorithmically track the prices of various virtual currencies and often leverage locked reserves of virtual currencies (or other digital assets). These locked reserves are known as "liquidity pools," and they are often used to facilitate trades. DEXs are built on blockchains that support smart contracts, including Ethereum, and often levy fees for their services.

11. Transaction Fee: A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions. Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (e.g., Bitcoin on the Bitcoin blockchain). On the Ethereum network, these transaction fees are called "gas fees." Gas fees are transaction costs paid in Ether, or its fraction, gwei. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion.

12. Stablecoins: Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S.

dollar, or to a different virtual currency. For example, Tether (also known as USDT) is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

13.Smart Contracts: Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

14.USDT and Tether Limited: Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

BACKGROUND ON CRYPTOCURRENCY CONFIDENCE SCAMS/PIG BUTCHERING SCAMS

15. Cryptocurrency confidence scams, commonly known as "Pig Butchering," are a type of internet-based cryptocurrency investment scam. The phrase is translated from Chinese shāzhūpán and refers to a scam in which the victim is "fattened up prior to slaughter." These scams are also referred to as cryptocurrency investment fraud.[1] These types of scams typically involved four stages. *First*, a perpetrator cold contacts a victim via text, social media, or some other communication platform. Oftentimes, the perpetrator will pretend to have contacted the wrong number but continue communicating with their newfound "friend." *Second*, the perpetrator will establish a relationship with the victim by continuing to message them over days, weeks, or months. *Third*, the scammer will concoct a narrative to induce the victim to send them a series of purported investments, often in the form of cryptocurrency. These payments are often made through fraudulent investment platforms introduced by the scammer, which the victim believes to be legitimate. *Fourth*, after the victim stops sending additional payments, or begins to question the scammer about legitimacy of their "investments," the perpetrator cuts off all contact.

---

[1] Federal Bureau of Investigation, *Cryptocurrency Investment Fraud,* https://www.fbi.gov/howwe-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrencyinvestment-fraud?__cf_chl_rt_tk=KP0jo5lKxpcHNmC2W9IgFvxzVp58YptXkC36h1AH84I-1749423762-1.0.1.1-PrqYwbOk3o56Boyjv4_oSFvOb0GH2RnyJMQVGilzVSs (Last accessed Jun. 17, 2025).

16. Confidence schemes are schemes where perpetrators gain trust or confidence from victims to deceive them into parting with their money. One of the most well-known forms of confidence schemes is the "romance scam," which typically features a perpetrator befriending a victim through the guise of a romantic relationship, often solely existing online, in an effort to siphon funds from the victim's bank accounts or assets.

17. Cryptocurrency confidence scams feature elements of well-established investment schemes blended with fraudulent websites, mobile apps, or dApps[2] and the opaqueness of cryptocurrency.

18. Law enforcement and independent investigations have determined that these schemes are perpetrated primarily in Southeast Asia, often via forced labor. Victims are trafficked into countries that include Myanmar, Philippines, Laos and Cambodia and are forced to conduct these scams via text messages, dating websites, and other online platforms inside scam compounds in these countries.[3]

19. In 2020—prior to the emergence of these types of scams—confidence schemes, or romance scams, were reported to have cost U.S. victims over $600 million dollars in losses. This represented a $125 million dollar increase from

---

[2] dApps are decentralized applications on blockchain networks, and typically are run on smart contracts.

[3] Cezary Podkul and Cindy Liu, *Human Trafficking's Newest Abuse: Forcing Victims into Cyberscamming*, https://www.propublica.org/article/human-traffickers-force-victims-intocyberscamming, (Sept. 13, 2022).

2019, and $238 million dollars from 2018, for a total of $1.43 billion dollars in losses attributed to confidence schemes from 2018–2020. Separately, during this same time-period, investment scams were reported to have cost U.S. victims over $800 million dollars.[4]

20. Since the emergence of cryptocurrency-based confidence scams, those same scam categories have seen their losses multiply at significant levels, reaching a reported loss of over $5.22 billion dollars in 2023 alone for confidence schemes and investments scams combined.[5] And in 2024, that same loss increased to approximately $7 billion dollars.[6] In 2024 alone, approximately $5.8 billion in losses from cryptocurrency investment fraud was reported to the Internet Crime Complaint Center.[7]

21. One of the primary attributes of this type of scheme, which has helped further its success, is the use of smartphone applications. 97% of Americans own a cellphone of some kind and nine-in-ten own a smartphone.[8]

---

[4] Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*, https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf, (Mar. 17, 2021).
[5] Federal Bureau of Investigation Internet Computer Complaint Center, *Internet Crime Report 2023,* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, (Apr. 4, 2024).
[6] Federal Bureau of Investigation Internet Computer Complaint Center, *Internet Crime Report 2024,* https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf, (Apr. 23, 2025).
[7] *Id.*
[8] Eugenie Park, Kaitlyn Radde, Michelle Faverio, Olivia Sidoti, Risa Gelles-Watnick, Sara Atske and Wyatt Dawson, *Mobile Fact Sheet,* https://www.pewresearch.org/internet/fact-sheet/mobile/ (Nov. 13, 2024).

22. Among the seemingly endless list of smartphone applications ("apps") are mobile banking or investment apps, which are typically associated with an individual's bank or investment account. These apps typically display an account owner's balance and transaction history, among other information. Notably, as of 2022, nearly 80% of Americans regularly use mobile banking apps or websites.[9]

23. Generally, information contained within legitimate mobile banking or investment apps, such as the balance, history, and interest, can be assumed by the user to be accurate. Furthermore, transactions performed on said legitimate app, reflected in the account history within the app, can generally be presumed to have occurred despite having no paper records like a receipt or statement one might receive if conducting the same transaction inside a brick-and-mortar institution.

24. This trust in mobile banking and investment apps is at the center of these schemes. Following the initial victimization through the confidence scheme, perpetrators convince victims to download what appear to be legitimate mobile banking or investment apps to track their cryptocurrency investments. In reality, they are not connected to any real account or legitimate financial institution.

---

[9] American Bankers Association, *National Survey: Record Number of Bank Customers Use Mobile Apps More Than Any Other Channel to Manage Their Accounts,* https://www.aba.com/about-us/press-room/press-releases/consumer-survey-banking-methods-2024#:~:text=The%20national%20survey%20found%20that,in%20the%20past%2012%20months. (Nov. 22, 2024).

Instead, the apps are created and controlled by the perpetrators, who are able to create the facade of balances and transactions that are otherwise non-existent.

25. This fabricated activity, which on the surface would appear no different than that of a legitimate mobile banking or investment app, is made to appear as though investments into non-existent, perpetrator-controlled platforms are realizing substantial gains. This helps the perpetrators convince victims into investing additional funds into the scheme.

26. Victims may contribute a small amount of funds to a cryptocurrency confidence scam, unwittingly, only to see those funds triple in value, as displayed on the perpetrator-controlled app. After this point, some victims attempt to invest more assets, which may include IRAs, 401(k)s, home equity loans, and college savings plans.

27. Some victims report being able to successfully withdraw funds which establishes trust and credibility with the perpetrators. This stage in the fraud scheme is designed to give the victims more confidence to invest their remaining assets. In these scenarios, what actually happens is that victims likely withdraw funds deducted from their "investments" (rather than purported gains), or originating from other victims and not a legitimate investment opportunity. This withdrawal ability deviates from more traditional confidence schemes and allows the scheme to continue for even longer.

28. Lastly, cryptocurrency confidence schemes most often involve cryptocurrency at the center of the investments. Cryptocurrency is well-known as a highly volatile asset, with price swings fluctuating the value of some cryptocurrencies, like Bitcoin, thousands of dollars in any given day. Cryptocurrency can also be highly technical, with terminology and attributes unique to different cryptocurrencies and blockchains. This has allowed for perpetrators to help convincingly explain convoluted investments to victims that otherwise would not consider purchasing or investing in cryptocurrency.

BACKGROUND OF THE SCAM PERPETRATED UPON CLAIMANT NO. ____

29. On or about June 8, 2022, the Claimant met an individual named Grace through a random text message.

30. After Claimant responded letting Grace know that she had the wrong number, she struck up a friendly conversation with the Claimant.

31. Grace moved the conversation to the encrypted messaging app Telegram.

32. After several days of building up trust, Grace introduced into the conversation the topic of investing in cryptocurrency.

33. Grace claimed to be an expert in trading cryptocurrency and told the Claimant she would mentor him and help him make significant profits from her trading methods.

34. Grace instructed Claimant into downloading Crypto.com where Claimant would purchase cryptocurrency and trade on a trading platform recommended by her called www.sbicoin.com.

35. Claimant was told that he would control the his cryptocurrency wallet held on www.sbicoin.com.

36. Despite its sophisticated appearance, www.sbicoin.com was not a legitimate platform and, unbeknownst to the Claimant, his wallet was controlled by the scammers.

37. A successful test run provided additional confidence to the Claimant that this fraudulent platform was legitimate.

38. Plaintiff began investing his assets transferred from Crypto.com to the fraudulent platform.

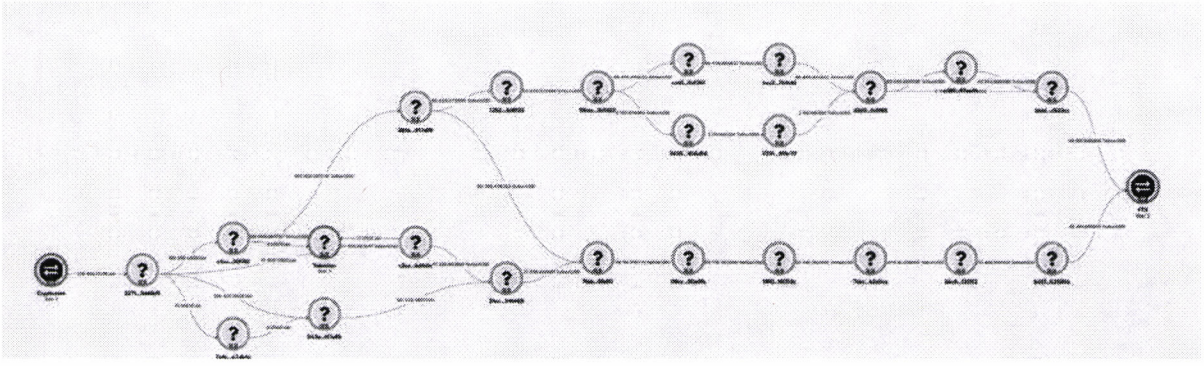
39. According to fraudulent statements, Plaintiff believed he was making significant profits. In total, Plaintiff invested more $518,000.00 in USDC which was transferred to the fraudulent investment platform. When Plaintiff believed his investment had more than doubled, he tried to withdrawal his profits.

40. When he was unable to successfully withdraw, Claimant was told he needed to pay taxes. This is when the Claimant realized he was a victim of a sophisticated cryptocurrency scam.

41. Using blockchain analytic tools, we have traced a portion of the Claimant's assets to the following deposit wallets held on the FTX exchange just prior to the FTX bankruptcy:

42. As reflected in the blockchain tracing report attached as Exhibit A, the Claimant sent his cryptocurrency from his Crypto.com wallet to 0x22711fc99eb8da1c4f065c114dfc2d56853d40d9, a wallet controlled by the perpetrators of this scam. After the Claimants stolen USDC was swapped at Tokenlon to USDT, the assets were laundered through a serious of intermediary wallets until 87,651 USDT was deposited in five transactions at the following FTX wallets:

- ddc1e66d5d8b749388db78797bb67e0e02641dac
- 2faf487a4414fe77e2327f0bf4ae2a264a776ad2



See Exhibit B – Full Tracing Graph.

43. The Claimant reported the theft to law enforcement and to the FBI. In or around Oct 2023, Detective Jeff Lomas notified FTX of the scam and served it with a seizure warrant which, unbelievably, FTX ignored. *See* Exhibit C – Email from Detective Lomas. Unbelievably, FTX ignored the seizure warrant. *Id.*

Acting pro se, the Claimant filed a proof of claim form. *See* Ex. D.

44. Despite the overwhelming proof provided herein and previously provided to FTX from the FBI Cyber Task force, the Debtor continues to refuse to assist the Claimant in recovering his stolen cryptocurrency and has objected to the Claimant's claim. Plaintiff respectfully requests the Court deny FTX's objection and order that Claimant be awarded $87,651 (USD) or 87,651 USDT.

Respectfully submitted,

By:

/s/ Daniel J. Thornburgh
Daniel J. Thornburgh
Aylstock, Witkin, Kreis
& Overholtz, PLLC
17 East Main Street
Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449
dthornburgh@awkolaw.com

Counsel for
CLAIMANT 93202

CERTIFICATE OF SERVICE

I, Daniel J. Thornburgh, hereby certify that the foregoing Claimant's Response in Opposition to the Debtors' 176th Omnibus Objection was filed with the United States Bankruptcy Court, 824 North Market Street, 3rd Floor, Wilmington, Delaware 19801, and a copy served on Counsel for Debtors and Debtors-in-Possession at landis@lrclaw.com, brown@lrclaw.com, pierce@lrclaw.com, dietdericha@sullcrom.com, bromleyj@sullcrom.com, glueckseinb@sullcrom.com, and kranzleya@sullcrom.com on July 11, 2025

By:

/s/ Daniel J. Thornburgh

Daniel J. Thornburgh
Aylstock, Witkin, Kreis
& Overholtz, PLLC
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449
dthornburgh@awkolaw.com

Counsel for CLAIMANT 93202